# CompTIA

## Exam Questions FC0-U61

CompTIA IT Fundamentals+ Certification Exam

**NEW QUESTION 1**
Which of the following can a company use to protect its logo?

A. Trademark
B. Copyright
C. Domain name
D. patent

**Answer:** A

**Explanation:**
A trademark is the best option for a company to protect its logo. A trademark is a name, symbol, logo, or slogan that identifies a product or service and distinguishes it from others in the market. A trademark grants the owner the exclusive right to use the mark and to prevent others from using confusingly similar marks. A trademark can be registered with the appropriate authority to obtain legal protection and enforcement. A trademark can last indefinitely as long as it is used and renewed periodically. A trademark can also be indicated by the symbols ™ or ®. A copyright is not suitable for protecting a logo, as it only protects original works of authorship, such as books, music, movies, or software. A domain name is not suitable for protecting a logo, as it only identifies a website or an email address on the internet. A domain name can be registered with a domain name registrar to obtain exclusive use of the name for a certain period of time. A domain name can also be trademarked if it meets the criteria for trademark protection. A patent is not suitable for protecting a logo, as it only protects inventions or processes that are new, useful, and non-obvious. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 8: Software Development Concepts

**NEW QUESTION 2**
A programmer needs an element that will automatically store customer orders consecutively by order number every time a new order is placed. Which of the following elements should be used?

A. Vector
B. Sequence
C. Array
D. Constant

**Answer:** B

**Explanation:**
A sequence is an element that will automatically store customer orders consecutively by order number every time a new order is placed. A sequence is a database object that generates sequential numbers according to a specified rule. A sequence can be used to create unique identifiers for records in a table, such as order numbers or customer IDs. A vector is an element that can store multiple values of the same data type in an ordered sequence, but it does not automatically generate sequential numbers. A vector is a data structure that can be used in programming languages such as C++ or Java. An array is an element that can store multiple values of the same data type in an indexed sequence, but it does not automatically generate sequential numbers. An array is a data structure that can be used in programming languages such as C or Python. A constant is an element that can store a single value of any data type that does not change during the execution of a program, but it does not automatically generate sequential numbers. A constant is a variable that can be used in programming languages such as C# or JavaScript. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 6: Database Fundamentals, Chapter 8: Software Development Concepts

**NEW QUESTION 3**
An online retailer experienced an outage. An investigation revealed that the server received more requests than it could handle, and customers could not log in as a result. Which of the following best describes this scenario?

A. Hardware failure
B. Denial of service
C. On-path attack
D. Social engineering

**Answer:** B

**Explanation:**
The scenario where an online retailer experienced an outage because the server received more requests than it could handle and customers could not log in as a result is best described as a denial of service. A denial of service is a type of attack that aims to disrupt or prevent the normal functioning or availability of a system or network by overwhelming it with excessive traffic or requests. A denial of service can cause performance degradation, slowdown, or outage for the system or network and its legitimate users. A denial of service can be performed by a single attacker or a group of attackers using multiple compromised devices, which is called a distributed denial of service (DDoS). A hardware failure is not the scenario that describes the online retailer's outage, but rather a possible cause or consequence of the outage. A hardware failure is a malfunction or breakdown of a physical component of a system or network, such as a disk, a memory, a CPU, a power supply, etc. A hardware failure can cause data loss, corruption, or interruption for the system or network and its users. A hardware failure can be caused by various factors, such as wear and tear, physical damage, overheating, power surge, etc. A hardware failure can also be induced by a denial of service attack that damages the hardware by overloading it. An on-path attack is not the scenario that describes the online retailer's outage, but rather a type of network attack that involves intercepting or modifying data packets that are transmitted between two parties on a network. An on-path attack can compromise the confidentiality, integrity, or authenticity of the data or communication between the parties. An on-path attack can be performed by an attacker who has access to the same network segment or device as one of the parties, such as a router, a switch, or a hub. An on-path attack can also be performed by an attacker who tricks one of the parties into sending data to them instead of the intended destination, which is called a man-in-the-middle attack. A social engineering attack is not the scenario that describes the online retailer's outage, but rather a type of attack that exploits human psychology and behavior to manipulate people into performing actions or revealing information that benefits the attacker. A social engineering attack can take various forms, such as phishing, vishing, baiting, quid pro quo, pretexting, or tailgating. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 7: Security Concepts

**NEW QUESTION 4**
Which of the following is an example of an interpreted language?

A. C++
B. Java
C. Python

D. Go

**Answer:** C

**Explanation:**
Python is an example of an interpreted language, which is a type of programming language that does not need to be compiled before execution. Instead, an interpreter program translates and executes the source code line by line at run time. Interpreted languages are usually easier to write and debug, but slower to execute than compiled languages. C++ and Java are examples of compiled languages, which are types of programming languages that need to be translated into executable machine code by a compiler program before execution. Compiled languages are usually faster to execute but harder to write and debug than interpreted languages. Go is an example of a hybrid language, which is a type of programming language that combines features of both compiled and interpreted languages. Hybrid languages use an intermediate code that can be executed by a virtual machine or an interpreter at run time. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 4: Programming Concepts and Data Structures, page 140.

**NEW QUESTION 5**
Meaningful and accurate reporting is essential to retailers in making business decisions while managing inventory. Which of the following offers the BEST assistance in generating reports?

A. Data capture and collections
B. Asset inventory inputs
C. Sales statistics
D. Average loss output

**Answer:** A

**Explanation:**
Data capture and collections are the processes of gathering and organizing data from various sources, such as transactions, surveys, sensors, etc. Data capture and collections would offer the best assistance in generating reports for retailers because they can provide accurate, relevant, and timely data that can be used for analysis and decision making. Asset inventory inputs, sales statistics, and average loss output are not processes that offer the best assistance in generating reports for retailers because they are not sources of data capture and collections, but rather types or results of data analysis. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 5: Database Fundamentals, page 200.

**NEW QUESTION 6**
A company will begin to allow staff to work from home by means of formal request. Which of the following is the BEST way for the company to document this change?

A. Written procedure
B. Written policy
C. Written email
D. Written memo

**Answer:** B

**Explanation:**
A written policy is the best way for a company to document a change that allows staff to work from home by means of formal request. A policy is a statement or guideline that defines the rules, standards, or procedures for an organization’s actions, decisions, or behaviors. A policy can help an organization to achieve its objectives, comply with regulations, ensure consistency and quality, and communicate expectations and responsibilities. A written policy is a policy that is documented in a formal document that can be distributed, reviewed, updated, and enforced by the organization. A written policy can help a company to document a change that affects its staff, such as working from home, by specifying the criteria, process, benefits, limitations, and consequences of the change. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 210.

**NEW QUESTION 7**
A user is getting an error message when trying to go to a website. A technician asks the user a few questions to find out more about the issue. The technician opens a browser locally and browses to the same site as the user. Which of the following troubleshooting steps is the technician using by browsing to the same site?

A. Establish a plan of action.
B. Gather information
C. Duplicate the problem.
D. Find the root cause.

**Answer:** C

**Explanation:**
The troubleshooting methodology is a systematic approach to solving problems that involves several steps, such as identifying the problem, establishing a theory of probable cause, testing the theory, establishing a plan of action, implementing the solution, verifying functionality, and documenting the findings. One of the steps in identifying the problem is to duplicate the problem, which means to reproduce the same error or issue that the user is experiencing. This can help the technician to verify the symptoms, narrow down the scope, and eliminate possible causes1011. References:= CompTIA IT Fundamentals (ITF+) Study Guide, 2nd Edition, Chapter 7: Explain the Troubleshooting Methodology4; Troubleshooting Methodology | IT Support and Help Desk | CompTIA12

**NEW QUESTION 8**
Which of the following best explains the reason for password expiration?

A. To disable unused user IDs
B. To invalidate any compromised passwords
C. To discourage writing down passwords
D. To enforce new password complexity rules

**Answer:** B

**Explanation:**
The best explanation for password expiration is to invalidate any compromised passwords. Password expiration is a security policy that requires users to change their passwords after a certain period of time, such as every 90 days. This reduces the risk of unauthorized access if an attacker obtains the user's password through phishing, hacking, or other means. If the user changes their password regularly, the old password becomes useless for the attacker. Password expiration does not necessarily disable unused user IDs, as the user may still be able to log in with their new password. Password expiration does not discourage writing down passwords, as some users may still do so to remember their new passwords. Password expiration does not enforce new password complexity rules, as those rules apply to any password change regardless of expiration. References: CompTIA IT Fundamentals (ITF+) Study Guide: Exam FC0-U61, Second Edition, Chapter 5: Database Fundamentals and Security Concepts, page 181

**NEW QUESTION 9**
A technician is concerned that sensitive data transmitted over the Internet can be intercepted and viewed during a MITM attack. Which of the following should the technician enable to reduce the risk?

A. DLP
B. ACL
C. TLS
D. IPS

**Answer:** C

**Explanation:**
TLS (Transport Layer Security) is a protocol that should be enabled to reduce the risk of a MITM
(man-in-the-middle) attack. A MITM attack is a type of cyberattack where an attacker intercepts and alters the communication between two parties without their knowledge. A MITM attack can compromise the confidentiality, integrity, and authenticity of the data being transmitted. TLS is a protocol that provides encryption, authentication, and integrity for data communication over the Internet. TLS can prevent a MITM attack by encrypting the data to make it unreadable by the attacker, authenticating the identities of the parties to prevent impersonation, and verifying the integrity of the data to detect any tampering. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 206.

**NEW QUESTION 10**
Which of the following is the most secure fllesystem?

A. FAT32
B. NFS
C. NTFS
D. exFAT

**Answer:** C

**Explanation:**
NTFS stands for New Technology File System, which is the most secure file system among the given options. NTFS is a file system that was developed by Microsoft for Windows operating systems. NTFS supports features such as encryption, compression, permissions, quotas, and auditing, which enhance the security and performance of the file system. FAT32 stands for File Allocation Table 32, which is a file system that was developed by Microsoft for older versions of Windows and DOS operating systems. FAT32 does not support encryption, compression, permissions, quotas, or auditing, and it has limitations on the size of files and partitions that it can handle. NFS stands for Network File System, which is a file system that was developed by Sun Microsystems for Unix and Linux operating systems. NFS allows users to access files on remote servers as if they were local files, but it does not support encryption or compression. exFAT stands for Extended File Allocation Table, which is a file system that was developed by Microsoft for flash drives and other removable media. exFAT supports larger files and partitions than FAT32, but it does not support encryption, compression, permissions, quotas, or auditing. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 4: Operating System Fundamentals

**NEW QUESTION 11**
A startup company has created a logo. The company wants to ensure no other entity can use the logo for any purpose. Which of the following should the company use to BEST protect the logo? (Select TWO).

A. Patent
B. Copyright
C. NDA
D. Trademark
E. EULA

**Answer:** BD

**Explanation:**
A logo is a graphical representation of a company's name, brand, or identity. A logo can be protected by both copyright and trademark laws. Copyright is a type of intellectual property that protects the original expression of ideas in tangible forms, such as books, music, art, or software. Copyright protects the logo from being copied, reproduced, or distributed without the permission of the owner. Trademark is a type of intellectual property that protects a word, phrase, symbol, or design that identifies and distinguishes the source of goods or services of one party from those of others. Trademark protects the logo from being used by other parties in a way that causes confusion or deception among consumers. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 211.

**NEW QUESTION 12**
Which of the following BEST describes a kilobyte?

A. A kilobyte is a measurement of storage (e.g., 100KB).
B. A kilobyte is a measurement of throughput (e.g.,100Kbps).
C. A kilobyte is a measurement of power (e.g., 100KW).
D. A kilobyte is a measurement of processor speed (e.g., 2.4KHz).

**Answer:** A

**Explanation:**

A kilobyte is a unit of digital information that equals 1,024 bytes. A byte is the smallest unit of data that can be stored or processed by a computer. A kilobyte can store a small amount of text, such as a few sentences or a paragraph. Storage devices, such as hard disks and flash drives, use kilobytes and other larger units, such as megabytes and gigabytes, to measure their capacity and performance. References: The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 38.

**NEW QUESTION 13**
A company wants an application to be accessed by concurrent users and store company information securely. Which of the following would be the BEST option for storing the information?

A. Word processing document
B. Flat file
C. Database
D. Spreadsheet

**Answer:** C

**Explanation:**
A database is a collection of data that is organized and stored in a way that allows easy access, manipulation, and analysis. A database would be the best option for storing information for an application that needs to be accessed by concurrent users and store company information securely. A database can handle multiple user requests, enforce data integrity and security, and perform complex queries and operations on the data. A word processing document, a flat file, and a spreadsheet are not options that can support concurrent users, store company information securely, or perform complex operations on the data. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 5: Database Fundamentals, page 191.

**NEW QUESTION 14**
Which of the following protocols is used to relay email from a user's mail server?

A. IMAP
B. FTP
C. SMTP
D. POP3

**Answer:** C

**Explanation:**
SMTP stands for Simple Mail Transfer Protocol, which is used to relay email from a user’s mail server to another mail server or from a mail client to a user’s mail server. IMAP stands for Internet Message Access Protocol, which is used to access and manage email messages on a mail server. FTP stands for File Transfer Protocol, which is used to transfer files between computers over a network. POP3 stands for Post Office Protocol version 3, which is used to download email messages from a mail server to a mail client. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 5: Infrastructure Concepts1

**NEW QUESTION 15**
Joe, a user, finds out his password for a social media site has been compromised. Joe tells a friend that his email and banking accounts are probably also compromised. Which of the following has Joe MOST likely performed?

A. Password reuse
B. Snooping
C. Social engineering
D. Phishing

**Answer:** A

**Explanation:**
Password reuse is the practice of using the same password for multiple accounts or services. Password reuse i a bad security habit that can lead to compromise of multiple accounts if one of them is breached by an attacker. Joe has most likely performed password reuse if he thinks his email and banking accounts are also compromised after his password for a social media site was compromised. Joe should use different passwords for different accounts and change them regularly to prevent password reuse. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 208.

**NEW QUESTION 16**
Which of the following would be BEST to keep the data on a laptop safe if the laptop is lost or stolen?

A. Host-based firewall
B. Strong administrator password
C. Anti-malware software
D. Full disk encryption

**Answer:** D

**Explanation:**
Full disk encryption would be the best way to keep the data on a laptop safe if the laptop is lost or stolen. Full disk encryption is a security technique that encrypts all the data on a hard drive, including the operating system, applications, and files. Full disk encryption prevents unauthorized access to the data without the correct password or key. Full disk encryption can protect the data on a laptop even if the laptop is physically removed or tampered with. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 203.

**NEW QUESTION 17**
A technician has successfully verified full system functionality after implementing the solution to a problem. Which of the following is the NEXT troubleshooting step the technician should do?

A. Determine if anything has changed.

B. Document lessons learned.
C. Establish a theory of probable cause.
D. Duplicate the problem, if possible.

**Answer:** B

**Explanation:**
Documenting lessons learned is the last step of the troubleshooting methodology, which is a systematic approach to solving problems. Documenting lessons learned involves recording the problem, the solution, and the process that was followed to resolve the problem. This can help prevent future occurrences of the same or similar problems, improve the troubleshooting skills of the technician, and provide a reference for other technicians who may encounter the same or similar problems. Documenting lessons learned would be the next troubleshooting step the technician should do after verifying full system functionality. Determining if anything has changed, establishing a theory of probable cause, and duplicating the problem are not steps that follow verifying full system functionality in the troubleshooting methodology. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 9: Troubleshooting and Operational Procedures, page 341.

**NEW QUESTION 18**
Which of the following is MOST likely used to represent international text data?

A. ASCII
B. Octal
C. Hexadecimal
D. Unicode

**Answer:** D

**Explanation:**
Unicode is the most likely encoding standard used to represent international text data. Unicode is a universal character set that can encode over a million characters from different languages, scripts, symbols, and emojis. Unicode supports multiple encoding forms, such as UTF-8, UTF-16, and UTF-32, that use different numbers of bytes to represent each character. Unicode enables consistent and interoperable representation and processing of text data across different platforms and applications. References : The Official CompTIA IT Fundamentals (ITF+) Study Guide (FC0-U61), page 138.

**NEW QUESTION 19**
A global variable called “age” will be created in a program and incremented through the use of a function. Which of the following data types should be defined with the age variable?

A. Integer
B. Float
C. Double
D. String

**Answer:** A

**Explanation:**
Integer is a data type that can store whole numbers, such as 1, 0, or -2. Integer would be the best data type to use for creating a variable to hold an age value because age is usually expressed as a whole number of years. Float, double, and string are not data types that would be suitable for creating a variable to hold an age value. Float and double are data types that can store decimal or fractional numbers, such as 3.14, 0.5, or -2.75. String is a data type that can store text or characters, such as “Hello”, “A”, or “123”. References: CompTIA IT Fundamentals+ Study Guide: Exam FC0-U61, Second Edition, Chapter 4: Programming Concepts and Data Structures, page 146.

**NEW QUESTION 20**
A corporate network just implemented a 60-day password-warning banner. Which of the following is most likely going to happen in 60 days?

A. Password reset
B. Password expiration
C. Password reuse
D. Password Implementation

**Answer:** B

**Explanation:**
The most likely thing that will happen in 60 days after implementing a 60-day password-warning banner is password expiration. A password-warning banner is a message that appears on the screen when a user logs in to a system or network, informing them of how many days are left before their password expires. A password expiration policy is a security measure that requires users to change their passwords periodically, usually every 30 to 90 days. This policy helps to prevent unauthorized access or compromise of passwords by hackers or malicious insiders. Password reset is the process of changing or creating a new password for a user account when the user forgets their password or wants to change it for security reasons. Password reset can be done by the user themselves or by an administrator, depending on the system or network settings. Password reset does not necessarily happen in 60 days after implementing a 60-day password-warning banner, unless the user forgets their password or chooses to change it before it expires. Password reuse is the practice of using the same password for multiple user accounts or systems. Password reuse is not recommended as it increases the risk of compromise if one of the accounts or systems is breached by hackers or malicious insiders. Password reuse does not necessarily happen in 60 days after implementing a 60-day password-warning banner, unless the user chooses to use their old password for their new password after it expires. Password implementation is not a term used in security, but it may refer to the process of creating or enforcing password policies for user accounts or systems. Password implementation does not necessarily happen in 60 days after implementing a 60-day password-warning banner, unless there are changes in the password policies that require users to comply with them. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam
FC0-U61), Chapter 7: Security Concepts1

**NEW QUESTION 21**
Which of the following actions is most likely associated with database use?

A. Creating diagrams

B. Querying
C. File sharing
D. Printing

**Answer:** B

**Explanation:**
The action that is most likely associated with database use is querying. Querying is the process of retrieving data from a database based on certain criteria or conditions. Querying allows users to access specific information from large amounts of data stored in tables. Querying can be done using SQL (Structured Query Language), which is a standard language for interacting with relational databases. SQL queries can perform various operations, such as selecting, inserting, updating, deleting, or joining data from tables. Creating diagrams is not an action that is associated with database use, but rather with software development or design. Creating diagrams can help visualize the structure, logic, or flow of a program or an algorithm. Examples of diagrams include flowcharts, UML diagrams, ER diagrams, etc. File sharing is not an action that is associated with database use, but rather with network use. File sharing is the process of allowing users to access or transfer files over a network. File sharing can be done using various protocols, such as FTP, SMB, NFS, etc. Printing is not an action that is associated with database use, but rather with output device use. Printing is the process of producing hard copies of documents, images, or other data on paper or other media using a printer. References: The Official CompTIA IT Fundamentals (ITF+) Student Guide (Exam FC0-U61), Chapter 6: Database Fundamentals1

**NEW QUESTION 22**
.....

# Thank You for Trying Our Product

## We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

## FC0-U61 Practice Exam Features:

* FC0-U61 Questions and Answers Updated Frequently

* FC0-U61 Practice Questions Verified by Expert Senior Certified Staff

* FC0-U61 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FC0-U61 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year